Ingeniería y competitividad
ISSN: 0123-3033
ISSN: 2027-8284
Facultad de Ingeniería, Universidad del Valle

Torres, Laura E.; Romero, Luis C.; Holguín, Erika P.; Ferro, Roberto; Aguirre, Edgar E.
Implementation of an IoT system for climate risk monitoring
Ingeniería y competitividad, vol. 24, no. 2, e20811356, 2022, July-December
Facultad de Ingeniería, Universidad del Valle

DOI: https://doi.org/10.25100/iyc.v24i2.11356

Available in: https://www.redalyc.org/articulo.oa?id=291374362007

How to cite
Complete issue
More information about this article
Journal's webpage in redalyc.org

Scientific Information System Redalyc
Network of Scientific Journals from Latin America and the Caribbean, Spain and Portugal
Project academic non-profit, developed under the open access initiative

ISSN: 0123-3033 – ISSN-e: 2027-8284
INGENIERIA Y COMPETITIVIDAD
REVISTA CIENTÍFICA Y TECNOLÓGICA
Vol. 24 No. 2-2022 – DOI: 10.25100/iyc.v24i2.11356

SYSTEM ENGINEERING

Implementation of an IoT system for climate risk monitoring

INGENIERÍA DE SISTEMAS

Implementación de un sistema de IoT para el monitoreo del riesgo climático

Laura E. Torres[1], Luis C. Romero[1], Erika P. Holguín[3], Roberto Ferro[1], Edgar A. Aguirre[12].

[1]Corporación Universitaria Minuto de Dios, Facultad de ingeniería, Bogotá, Colombia

[2]Universidad Distrital Francisco José de Caldas, Bogotá, Colombia

[3] Colsubsidio Educación Tecnológica -CET, Bogotá, Colombia

ltorres@uniminuto.edu, lromero@uniminuto.edu, erika.holguin@cetcolsubsidio.edu.co, rferro@udistrital.edu.co, eaguirre@uniminuto.edu

Recibido: 8 de junio de 2021 – **Aceptado**: 2 de noviembre de 2021

Abstract

The data collected in vulnerability and risk scenarios, in the context of prevention of natural disasters, are the basis for consolidating information that allows having the elements to mitigate the impact of the natural aspects that generate the risk; In this sense, when a system is structured where the data associated with variables that measure or monitor particular natural aspects are captured, stored and transformed, there is a need to secure these data to optimize the fidelity of the information. The results of the research presented are focused on the development of an Internet of Things (IoT) system for monitoring climate risk, through sensors connected remotely and whose data is processed for the generation of statistical reports. descriptive such as calculation of the mode, mean, median; minimum, and maximum that facilitate the understanding of the monitored variables.

Keywords: *Internet of things, web services platform, reports, data analytics, risk management.*

Como citar:
Torres LE, Romero LC, Holguín EP, Ferro R, Aguirre EA. Implementación de un sistema de IoT para el monitoreo del riesgo climático. *INGENIERÍA Y COMPETITIVIDAD*, 2022; e20811356. https://doi.org/10.25100/iyc.v24i2.11356.

Este trabajo está licenciado bajo una Licencia Internacional Creative Commons Reconocimiento–NoComercial–CompartirIgual 4.0

Resumen

Los datos que se recolectan en escenarios de vulnerabilidad y riesgo, en el contexto de prevención de desastres naturales, son la base para consolidar información que permite disponer de los elementos para mitigar el impacto de los aspectos naturales que generan el riesgo; en tal sentido, cuando se estructura un sistema donde se capturan, almacenan y transforman los datos asociados con variables que miden o monitorean aspectos naturales particulares, se presenta la necesidad de asegurar esos datos para optimizar la fidelidad de la información. Los resultados de la investigación que se presenta se centran en el desarrollo de un sistema de internet de las cosas (IoT, por sus siglas en inglés) para el monitoreo del riesgo climático, a través de sensores conectados de forma remota y cuyos datos se procesan para la generación de reportes estadísticos descriptivos como cálculo de la moda, media, mediana; mínimo y máximo que facilitan la comprensión de las variables monitoreadas.

Palabras Clave: *Internet de las cosas, plataforma de servicios web, reportes, analítica de datos, gestión de riesgos.*

1. Introducción

La gestión del riesgo se enfoca en tres procesos: conocimiento del riesgo, reducción de riesgo y manejo de desastres; la naturaleza del presente trabajo aborda el proceso de conocimiento del riesgo a través de la construcción de una plataforma de Internet de las Cosas (IoT), como elemento de un sistema de alertas tempranas que permite la recolección de datos provenientes de diferentes sensores.

Los Sistemas de Alerta Temprana SAT [(1)] han venido desarrollándose y fortaleciendo en los últimos años [(2)] y se han enfocado en emergencias derivadas de desastres naturales como terremotos, inundaciones, deslizamientos e incendios y actualmente, por el impacto del cambio climático se enfocan en la recolección de variables ambientales.

El auge y crecimiento de las plataformas orientadas al IoT superan más de 39 aplicaciones de tratamiento formal de datos [(3)], lo cual implica la necesidad del tratamiento de grandes volúmenes de datos haciendo uso del paradigma de almacenamiento en la nube. Lo anterior ha llevado a que surjan empresas privadas que ofrecen la posibilidad de desarrollar sistemas orientados al IoT, arquitectura global emergente de la información basada en Internet que facilita el intercambio de bienes y servicios en las redes desde cualquier lugar geográfico del mundo con acceso a Internet [(4)].

En el contexto colombiano, se observa la implementación de plataformas para el registro de datos donde se almacena y administra la información para generar análisis y reportes estadísticos que permiten conocer el riesgo de diferentes eventos para la toma de decisiones y mitigación de riesgos naturales. Tales acciones se desarrollan en entidades del estado como: el Instituto de Hidrología, Meteorología y Estudios Ambientales IDEAM [(5)], el Instituto Distrital de Gestión de Riesgos y Cambio Climático IDIGER [(6)] y la Unidad Nacional para la Gestión del Riesgo de Desastres UNGRD [(7)]; así como en grupos de investigación de distintas universidades de carácter público y privado.

Lo descrito se convierte en un punto clave a la hora de implementar este tipo de sistemas, debido a que muchas de las empresas que incorporan el paradigma de almacenamiento en la nube tienen sus servidores de recepción y almacenamiento de datos distribuidos en varios países del mundo [(3)], y donde contratan a terceros que les prestan servicios que no permiten que el titular de la información conozca la ubicación real de los datos y por tanto, si está cediendo la titularidad de los mismos [(8)]. Sí el titular en algún momento desea migrar su información podría tener conflictos por las políticas de tratamiento de datos de cada país.

Como consecuencia de lo anterior y dada la escasa cultura de protección de la información [(9)]

por parte del titular, se produce la cesión no consciente de la información a cualquier organización que le ofrezca los servicios de almacenamiento, para sus dispositivos de IoT sin antes evaluar sus políticas de protección y tratamiento de datos [8].

Es por lo anterior, que se hace necesario la implementación de una plataforma que garanticen la integridad de los datos, la pregunta de investigación guía planteada en esta investigación fue ¿cómo desarrollar un sistema de IoT que permita el monitoreo del riesgo climático?

De acuerdo con lo descrito y para realizar un sondeo de opinión se aplicó una encuesta entre los usuarios de plataformas IoT en el departamento de informática y electrónica de la corporación universitaria minuto de Dios que tiene 65 profesores, tomando como muestra a 24 profesores siendo el tamaño de la muestra del 36.92% los cuales respondieron a la pregunta: ¿cree usted que se hace necesario la implementación de una plataforma en donde se garantice la integridad y titularidad de los datos? de acuerdo con las siguientes opciones, si 91,3% y no el 8,7%, se determina desde el resultado cuantitativo, que un número significativo de profesores (21 de 23 profesores encuestados) considera necesaria la implementación de una plataforma donde se garantice la integridad y titularidad de los datos, dado que las plataformas de IoT donde implementan sus proyectos no les permiten tener acceso completo de la información. En consecuencia, se presentan obstáculos para que la investigación cumpla con los objetivos planteados.

Un elemento importante para un usuario es leer detenidamente los acuerdos de licencia y políticas de tratamiento de datos establecidos por cada compañía, dado que sin hacer una evaluación de las cláusulas a las cuales se somete el usuario al aceptar el acuerdo, puede ceder la titularidad de los datos, a través del instrumento de encuesta aplicado a los investigadores, se encontró que sólo el 31.6% de los profesores evalúan las políticas de protección y tratamiento de datos, mientras que el 68.5% no lo hacen o identifican las políticas limitadamente, en algunas ocasiones, pregunta número tres: antes de aceptar los términos de licencia para el uso de una plataforma orientada al IoT, ¿evalúa las políticas de protección y tratamiento de datos que allí se plantean?.

Por lo anterior, el objetivo de esta investigación ha sido desarrollar un sistema de IoT que permita el monitoreo del riesgo climático atreves de la recepción, almacenamiento, presentación y análisis estadístico de variables ambientales como la temperatura, humedad relativa y otros que permitan conocer el riesgo de diferentes eventos, para reportar métricas de información generadas por sensores, analizando diferentes metodologías, componentes y tecnologías que se utilizan para plataformas de IoT, así se determinan las historias de usuario para realizar la recepción, almacenamiento, presentación y análisis de datos, finalizando con el diseño una base de datos para el almacenamiento y administración de datos suministrados por sensores teniendo en cuenta el tratamiento de la información de la titularidad.

Los antecedentes se realizaron a través de un análisis del estado del arte donde se encontraron trabajos relacionados con el diseño de sistemas de redes de sensores inalámbricos para aplicaciones de monitoreo ambiental, donde se describen sistemas de redes de sensores inalámbricos que los autores han desarrollado utilizando diferentes plataformas de hardware. El énfasis de las diferentes investigaciones se centró en desarrollar sistemas de bajo costo y altamente escalable, en cuanto al tipo de sensores, como al número de nodos sensores, lo que lo hace muy adecuado para una amplia variedad de aplicaciones relacionadas con el monitoreo ambiental y la gestión del riesgo [10].

El área de la seguridad, privacidad y confianza en internet de las cosas es tratado por [11]. donde propone un escenario de IoT buscando la satisfacción de los requisitos de seguridad y privacidad que desempeñan un papel fundamental. Estos requisitos incluyen confidencialidad y autenticación de datos, control de acceso dentro de la red de IoT, privacidad y confianza entre usuarios y cosas, y la aplicación de las políticas de seguridad y privacidad, las contramedidas de seguridad tradicionales no pueden aplicarse directamente a las tecnologías IoT [12] debido a los diferentes estándares y protocolos de comunicación, además el elevado número de dispositivos interconectados plantea problemas de escalabilidad, por lo tanto es necesaria una infraestructura flexible capaz de hacer frente a las amenazas [13] de seguridad [14] de en un entorno tan dinámico.

2. Metodología

Para alcanzar el objetivo se determinaron puntos de interés relevantes para el sistema de información, iniciando por un levantamiento de insumos a través de consultas en jornadas de trabajo con profesores que usan plataformas de IoT, esta etapa del proyecto permitió analizar componentes, tecnologías para la estructuración de historias de usuario y como contraste se realizó una búsqueda de antecedentes.

La siguiente etapa consistió en el análisis, diseño, desarrollo e implementación del sistema, en la etapa de diseño se levantaron los requerimientos funcionales y no funcionales para el sistema de información, además de determinaron los requerimientos conceptuales, normativos y legales.

En la etapa de diseño se elaboraron los diseños previos de los modelos conceptuales y físicos de la base de datos del sistema de información basados en la información de la etapa de análisis, así mismo se elaboraron los diagramas de casos de uso, diagramas de secuencia y diagramas de despliegue, adicionalmente se llevó a cabo la documentación de los casos de uso, el modelo entidad relación fue elaborado para dar paso a la construcción del diccionario de datos y el modelo relacional; en base a lo descrito anteriormente, fue posible desarrollar la base de datos, contando con el esquema de datos, se inició la elaboración de mockups del sistema y se procedió con la codificación a nivel de FrontEnd y BackEnd.

En la etapa de desarrollo se instalaron los ambientes, se creó la base de datos teniendo en cuenta la administración de recursos de máquina, velocidad de registro y lectura de datos, a partir de la construcción del ambiente se inició con los procesos específicos de desarrollo del sistema de información con sus funcionalidades de acuerdo con las historias de uso y/o casos de uso definidos en la etapa de análisis.

Durante la etapa de implementación para la puesta en producción se verifico la plataforma tecnológica para la implementación del sistema y se puso en marcha cada una de las funcionalidades del sistema, finalmente la puesta en producción verificó la implementación total de las historias de usuario, se comprobó que el sistema estuviese listo para ser entregado al usuario y finalmente se documentaron errores.

La puesta en producción verificó la implementación total de las historias de usuario, se comprobó que el sistema estuviese listo para ser entregado al usuario y finalmente se documentaron errores.

3. Modelo

El modelo general se describe bajo tres elementos, Figura 1; el primer elemento es la conexión de dispositivos, el segundo elemento es el procesamiento de datos, análisis y administración, y el tercer elemento es la presentación. A continuación, se describen en detalle cada uno de los elementos.

La conexión de dispositivos contiene los nodos sensores que son los encargados de la captura de los datos en tiempo real y luego enviarlos a través de la red al broker MQTT, el cual se encarga de recibir los datos de cada nodo, se usaron ocho sensores de humedad y temperatura, de los cuales cuatro son dht11 y cuatro son dht21 para pruebas experimentales, teóricamente el bróker y la red soporta 30 conexiones simultaneas.

Una vez los datos llegan al broker MQTT, se ejecuta un script de Python que se conecta al broker MQTT y extrae los datos para posteriormente enviarlos a la base de datos y ser almacenados. Luego, a través de API RESTFULL se realizan transacciones con la base de datos, generando reportes con analítica descriptiva.

Por medio de dispositivos móviles con conexión a Internet se realiza la presentación, donde fue posible visualizar los datos que fueron capturados por los nodos sensores y a través de una analítica se generaron alertas en tiempo real, así como reportes históricos y cálculos estadísticos haciendo uso de interfaces web responsive.

La arquitectura propuesta en la Figura 2 para el sistema consta de tres elementos principales, iniciando por la conexión de dispositivos, en donde se integran los nodos sensores, los cuales capturan dos variables meteorológicas (temperatura y humedad relativa) y se conectan a la red mediante tecnología WiFi, para luego enviar estos datos al broker MQTT, la aplicación cliente (MVC) consume los servicios a través de tecnología AJAX, los procesa y presenta a través de tres vistas denominadas: dash board, históricos y alertas

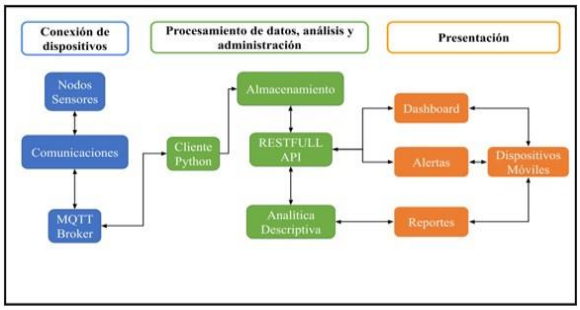

***Figura 1**: modelo general del sistema*

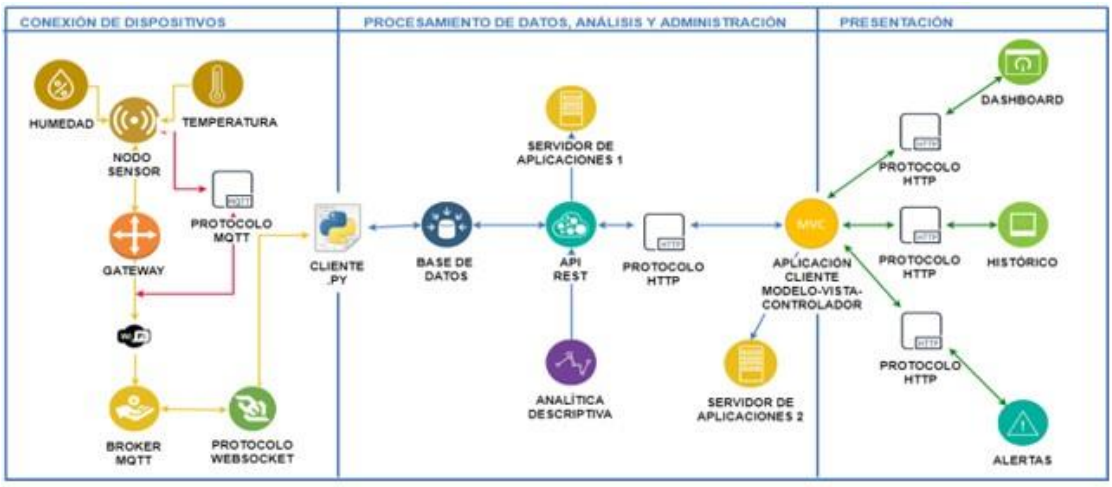

***Figura 2** Arquitectura plataforma IoT.*

El sistema gestor de base de datos usado es MariaDB versión 10.2, motor virtualizado en una máquina en Amazon Web Service (AWS) con sistema operativo Windows Server 2016 Datacenter. El modelo relacional de la base de datos se compone de once tablas dentro de las

cuales la tabla dato contiene la unidad de medida y el dato capturado; la tabla en mención está relacionada con el dispositivo para identificar de cuál de los dispositivos proviene cada dato.

El modelo de base de datos es relacional Figura 3 debido a que la integridad referencial garantiza la actualización de la información en todas las tablas, en tiempo real, para minimizar la pérdida de información dadas las intermitencias que se presentan en los servicios de red. Lo anterior se ha asegurado a través del proceso de modelamiento e implementación de la base de datos siguiendo la estructuración de un diseño con etapas de modelamiento entidad-relación y de la aplicación de la normalización hasta tercera forma normal, para así, generar el modelo relacional a implementar en el sistema gestor MariaDB versión 10.2.

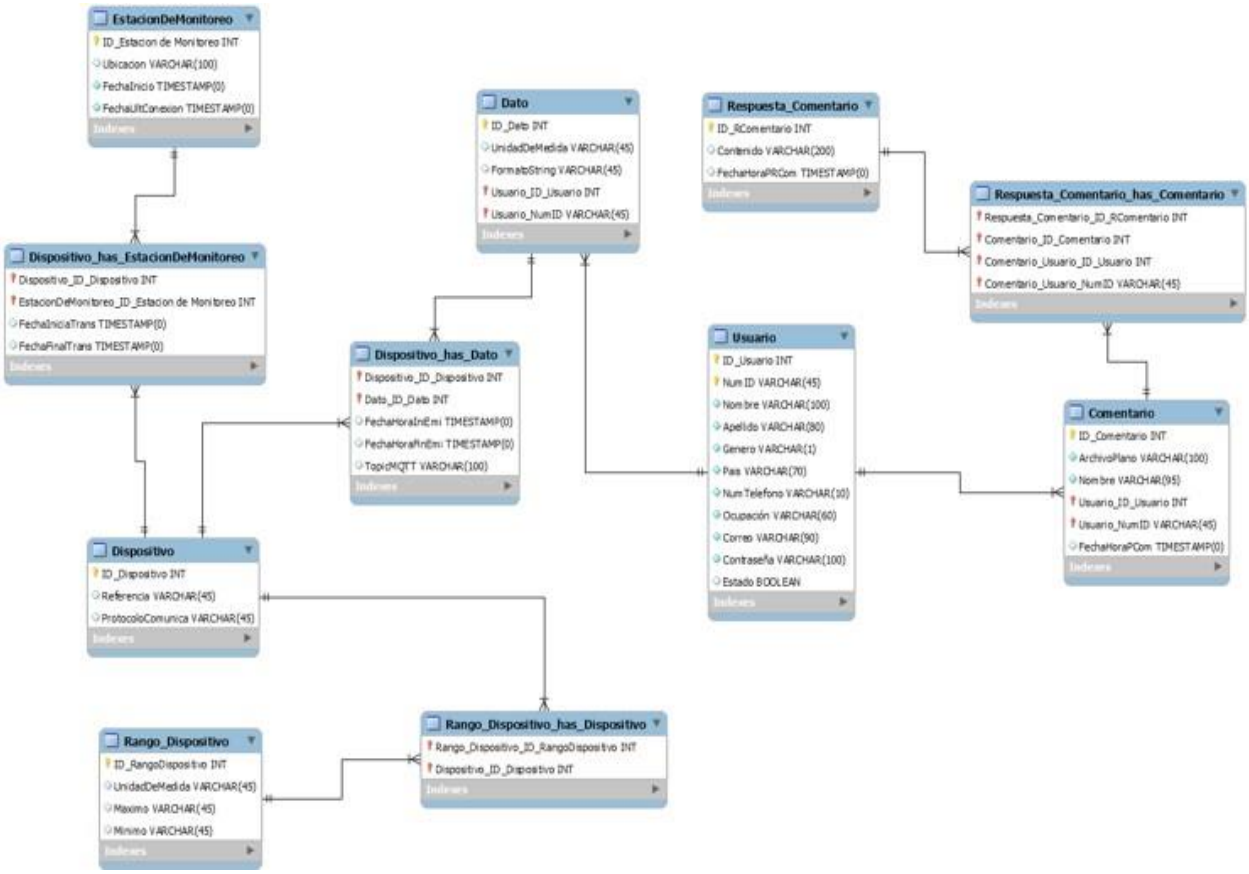

Figura 3 *modelo relacional de la base de datos*

Como se observa en la Figura anterior, cada tabla contiene los campos para almacenar los datos que permiten la generación de los reportes de visualización del comportamiento de las variables capturadas por los sensores.

4. Resultados

Se logró implementar el sistema de IoT para el monitoreo del riesgo climático; la interfaz que se observa en la Figura 4 muestra una arquitectura que contó con la conexión de dispositivos por medio de una estación de monitoreo. Así mismo, la implementación cuenta con el procesamiento, análisis y administración de un sistema con componentes de hardware y software que permiten presentar visualmente, la información almacenada. A continuación, se muestra la

interfaz de bienvenida del componente de software del sistema:

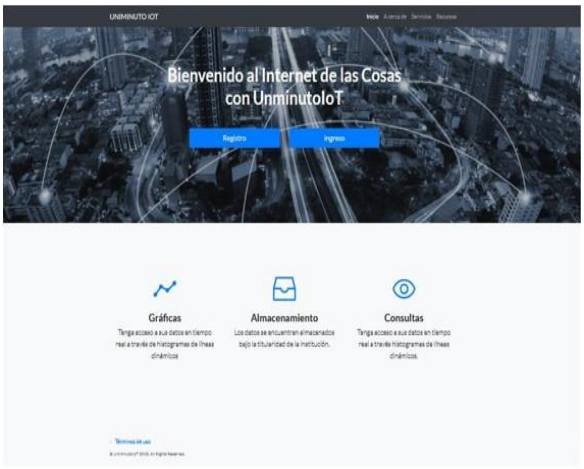

Figura 4 *sistema de IoT para el monitoreo del riesgo climático*

Los resultados de la plataforma se obtuvieron por medio de un conjunto de pruebas de conexión de diferentes estaciones de monitoreo con un conjunto de sensores para enviar datos y poder ser almacenados. Las pruebas contemplaron la visualización de los datos capturados por los sensores a través de gráficos de líneas en tiempo real, la consulta de datos históricos de variables para visualizarlos en un gráfico de área, los reportes estadísticos básicos sobre los datos históricos (cálculo de la moda, media, mediana; mínimo y máximo), los reportes gráficos del comportamiento de los datos con mapas de calor y la visualización de alertas en tiempo real cuando un dato se encuentra fuera de un umbral previamente configurado. A continuación, se describen detalladamente los resultados:

A través de los gráficos dinámicos que se observan en la Figura 5, se representan en tiempo real los datos capturados por la estación de monitoreo, estos se visualizan con el valor, la fecha y hora del dato capturado en el servidor. Una característica de la aplicación es que el gráfico permite realizar un filtro de los datos en periodos de tiempo divididos en tres secciones: un minuto, cinco minutos y todos los datos que fueron censados.

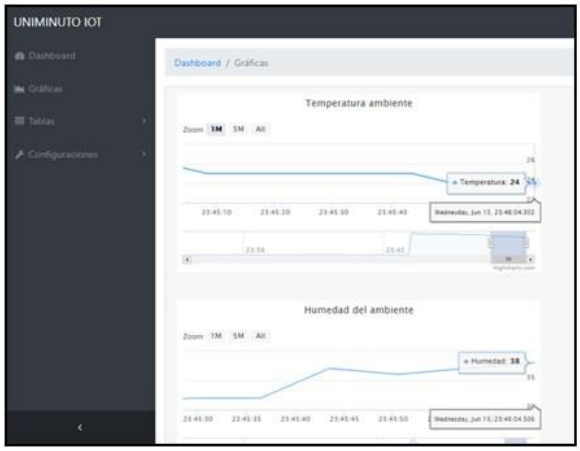

Figura 5 *Representación dinámica de datos capturados*

Por medio de una consulta parametrizada del tipo de variable, la fecha, la hora inicial, hora final y selección de estación de monitoreo, se generó un gráfico de área que muestra el conjunto de datos consultados para humedad como se ve en la Figura 6, y de datos de temperatura como se observa en la Figura 7. Adicional, se ilustra el comportamiento de las variables en días, semanas, meses y año, detallando el valor del dato, la fecha y la hora, lo cual permite exportarlos en formato Microsoft Excel™.

.

Figura 6 *Consulta histórica de humedad relativa.*

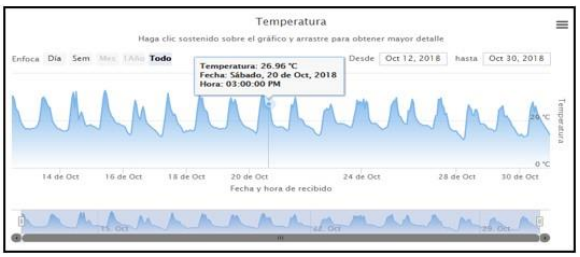

Figura 7 *Consulta histórica de temperatura.*

La plataforma cuenta con dos tipos de consulta, Figuras 8 y 9, las cuales muestran los datos a través de las medidas de moda, media y mediana, mínimo y máximo, así como a través de gráficos de barras diferenciados por color y una columna que incluye el detalle de la consulta.

Adicionalmente, como se visualiza en la Figura 10, se genera una Figura denominado mapa de calor que se obtiene a partir de una consulta parametrizable de las variables: fecha, hora inicial, hora final y estación de monitoreo. La Figura presenta la concentración de datos discriminados por color, con la finalidad de identificar las franjas de tiempo con mayor o menor valor de una variable.

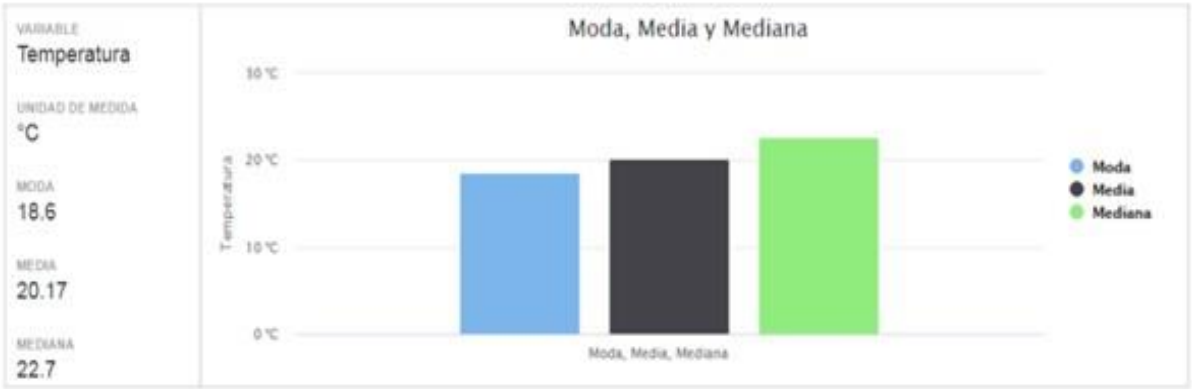

Figura 8 *Consulta estadística moda, media y mediana.*

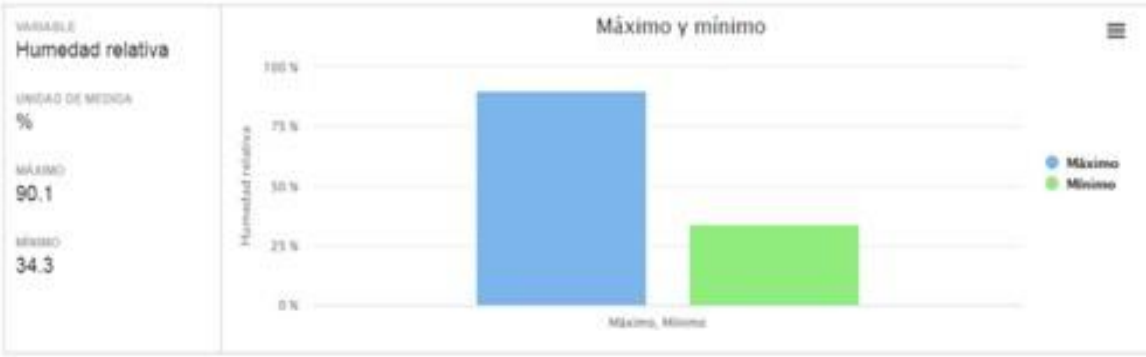

Figura 9 *Consulta estadística máximo y mínimo*

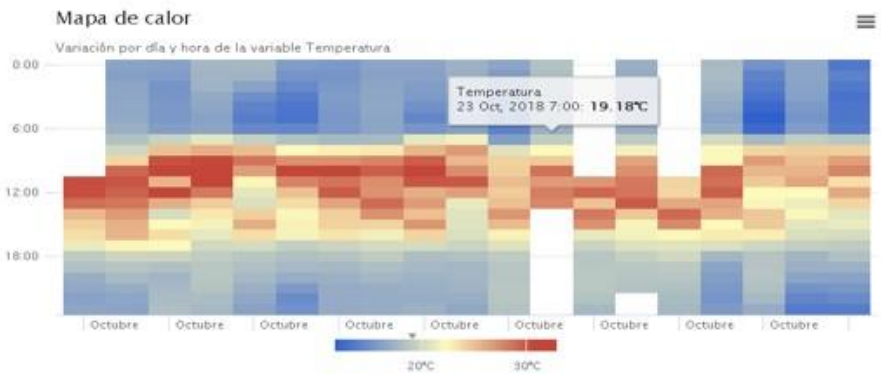

Figura 10 *Mapa de calor variable temperatura.*

Las alertas en tiempo real, Figura 11, se obtienen a partir de umbrales previamente configurados, los cuales se comparan con el dato que es capturado y almacenado. Si este dato se encuentra fuera del umbral se dispara una alerta que se muestra en el Dash Board indicando la variable, la estación, el dato y la fecha y hora.

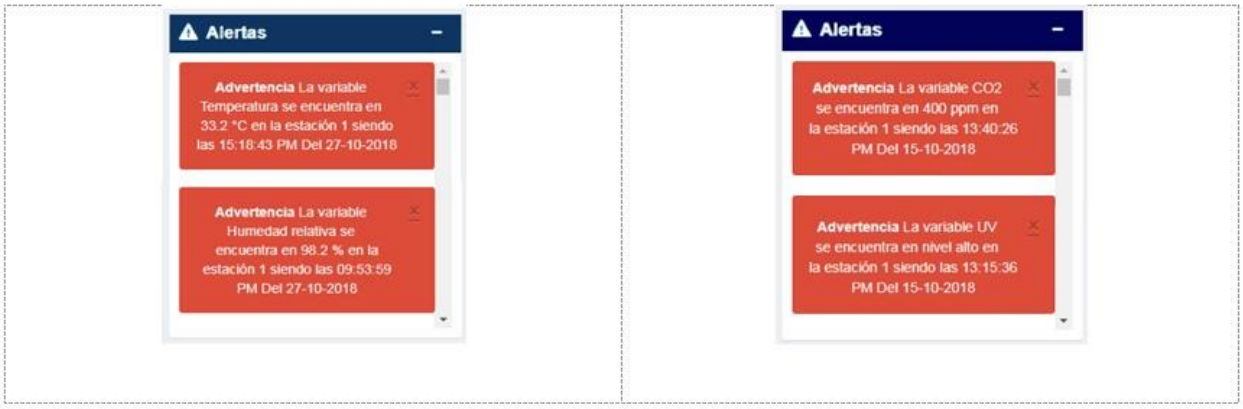

Figura 11 *Vista de alertas.*

5. Conclusiones

Se implementó el sistema de IoT descrito en el presente artículo con resultados correctos de funcionamiento, debido a que adicional a la cohesión técnica y tecnológica entre los componentes de software y hardware del sistema, es posible visualizar los datos de sensores climáticos; además, se comprueba que el módulo de analítica posibilita la comprensión del comportamiento de las variables a través de las diferentes opciones estadísticas como la moda, media y mediana de los datos capturados, y el mapa de calor permiten representar posibles comportamientos.

La conexión de sensores al sistema no es compleja pero se debe aclarar que por el tipo de infraestructura usada se implementó el protocolo de comunicaciones; tal elemento de sincronización y monitoreo de la comunicación es un factor elemental para asegurar el funcionamiento de un sistema que tiene componentes de hardware y software, sobre todo

cuando se trata de un caso de infraestructura propia y donde es fundamental evaluar las implicaciones del tipo de organización, debido a las particularidades de las políticas de seguridad y los cambios o ajustes que deben aplicarse como sucede con protocolos como MQTT, que implican el uso otro tipo de protocolos de conexión.

Los tiempos de conexión al servidor variaron dependiendo de la red usada, aunque al tratarse de datos de tamaño mínimo, en algunos momentos de intermitencia del servicio, se perdieron. Para un trabajo futuro, en este apartado es fundamental la prueba de calidad y estabilidad del servicio, de modo que sea posible probar los protocolos de comunicaciones con diferentes cargas de datos y en diferentes infraestructuras de comunicaciones. En el proceso presente, la carga computacional de la tarjeta de desarrollo usada para transmitir datos fue suficiente porque sólo se usó como un dispositivo de IoT para la adquisición y transmisión de datos.

El módulo de estadística permite tener una mirada general del comportamiento de las variables, aunque se debe tener cuidado con el tipo de estadística usada frente el tipo de variable y el contexto. Por ejemplo, al experimentar en situaciones ambientales cotidianas se observó que los cambios de temperatura y humedad relativa no son drásticos y en algunos periodos seguidos de tiempo la variable no tiene alteraciones; lo anterior generó cuestionamiento a los autores respecto al proceso de transmisión de datos cuando estos no han variado, teniendo en cuenta los costos computacionales asociados a la continua transmisión de los mismos.

Se observó que el módulo de estadística no es suficiente para otros escenarios; en el caso particular, el sistema permite la detección de riesgos frente a variables máximas y mínimas, pero carece de un proceso de predicción, por lo cual, otro posible trabajo futuro es el desarrollo de componentes de predicción para escenarios de riesgo específicos.

6. Referencias

(1). PNRRD | ONEMI: Ministerio del Interior y Seguridad Pública -ONEMI: Ministerio del Interior y Seguridad Pública - [Internet]. 2021 [citado 24 de octubre de 2021]. Disponible en: https://www.onemi.gov.cl/plataforma-de-reduccion-de-riesgos-de-desastres/

(2). IDIGER. Sistema de Alerta Temprana en funcionamiento de los salgareños [Internet]. 2017 [citado 23 de febrero de 2017]. Disponible en: http://portal.gestiondelriesgo.gov.co/Paginas/Noticias/2016/El-SAT-Sistema-de-Alerta-Temprana-en-funcionamiento-de-los-salgarenos.aspx

(3). Mineraud J, Mazhelis O, Su X, Tarkoma S. A gap analysis of Internet-of-Things platforms. Comput Commun [Internet]. 4 de febrero de 2016 [citado 16 de abril de 2021];89–90:5–16. Disponible en: http://arxiv.org/abs/1502.01181

(4). Weber RH. Internet of Things - New security and privacy challenges. Comput Law Secur Rev. 1 de enero de 2010;26(1):23–30.

(5). Ramos C AM, Trujillo-Vela MG, Prada S LF. Análisis descriptivos de procesos de remoción en masa en Bogotá. Obras y Proy [Internet]. diciembre de 2015 [citado 23 de febrero de 2017];(18):63–75. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-28132015000200006&lng=en&nrm=iso&tlng=en

(6). Climático nstituto D de G de R y C. Inicio - Idiger [Internet]. 2021 [citado 16 de abril de 2021]. Disponible en: https://www.idiger.gov.co/

(7). UNGRD. Unidad Nacional para la Gestión del Riesgo de Desastres [Internet]. 2019.

Disponible en: http://portal.gestiondelriesgo.gov.co

(8). España. Ministerio de Industria T y C. Boletín económico de ICE, información comercial española. Boletín económico de ICE, Información Comercial Española, ISSN 0214-8307, No 3070 (Del 1 al 31 de Diciembre 2015), 2015, págs. 27-36. Servicio de Publicaciones; 1999. 27–36 p.

(9). Vallejo M. Kids and parents privacy exposure in the internet of things: How to protect personal information. Comput y Sist. 2018;22:1191–205.

(10). Bravo BA, Luis G, Belduma Belduma A, Johnatan IE, González C. Seguridad, privacidad y confianza en Internet de las cosas: El camino por delante. 2017.

(11). Gonzalez M. Internet de las cosas: Seguridad, privacidad y protección [Internet]. Mundo Digital. 2015 [citado 16 de abril de 2021]. Disponible en: https://www.bbvaopenmind.com/tecnologia/mundo-digital/internet-de-las-cosas-seguridad-privacidad-y-proteccion/

(12). Su J, Cao D, Zhao B, Wang X, You I. ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the Internet of Things. Futur Gener Comput Syst. abril de 2014;33:11–8.

(13). Jorge Pérez EB. El debate sobre la privacidad y seguridad en la red: regulación y mercados [Internet]. Ariel E, editor. Barcelona; 2012. Disponible en: https://universoabierto.org/2016/01/28/el-debate-sobre-la-privacidad-y-seguridad-en-la-red-regulacion-y-mercados/

(14). MinTic. G.ST.02 Guía de Computación en la nube - Arquitectura TI. 2018 [citado 16 de abril de 2021];44. Disponible en: https://www.mintic.gov.co/arquitecturati/630/w3-article-75554.html